UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	17 Cr. 560 (JMF)
ZHENGQUAN ZHANG, a/k/a "Zheng Quan Zhang," a/k/a "Jim Z. Zhang,"	:	
Defendant.	:	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
Attorney for the United States of America

Eun Young Choi
Won S. Shin
Assistant United States Attorneys
Of Counsel

Table of Contents

Table of Authorities

Cases

Other Authorities

The Government respectfully submits this memorandum of law in opposition to defendant Zhengquan Zhang's motion to suppress. This Court should deny Zhang's motion in its entirety.

I. Background

A. The Indictment

Firm-1 is a global financial services firm headquartered in New York, New York, that engages in the trading of publicly traded securities and other financial products. Firm-1 uses proprietary algorithmic trading models to help it predict market movements and make trading decisions (the "Trading Models"). In addition, Firm-1 uses proprietary trading platforms to create, submit, and execute orders on exchanges and market centers (the "Trading Platforms"). (Indictment 17 Cr. 560 (JMF) (the "Indictment") ¶ 1).

These Trading Models and Trading Platforms contribute substantially to Firm-1's market share and profits. Because of the competitive advantages and economic value that Firm-1 derived from these assets, Firm-1 has put in place substantial measures designed to protect the computer source code that comprise the Trading Models and Trading Platforms from disclosure to a competitor or to the public. These measures include, among other things, the use of encryption keys to restrict employee access to the data, restrictions on the ability to download data to storage devices, and employee confidentiality agreements. (Indictment ¶ 4).

Firm-1 employed defendant Zhengquan Zhang in technical roles; he was initially based in the greater New York City area and was later based in Firm-1's San Jose, California office. (Indictment ¶ 2). From at least December 2016 through March 2017, Zhang orchestrated a scheme to steal from Firm-1 both proprietary data, including various Trading Models and Trading Platforms, as well as confidential data associated with other Firm-1 employees, including email data. In furtherance of this scheme, Zhang purposely circumvented efforts by Firm-1 to protect its

data from theft, including through the use of network infrastructure located in this District and elsewhere. (Indictment ¶ 3).

For example, Zhang installed on Firm-1's system computer code designed to look for encryption keys to gain access to encrypted portions of the Trading Models. Zhang also modified an application on Firm-1's system to steal the usernames and passwords of other Firm-1 employees to gain access to their email data. Zhang used an area of Firm-1's computer system to store millions of files of data, including unencrypted portions of the source code of the Trading Models and email data for other Firm-1 employees, to which Firm-1 had not granted Zhang access. Zhang sent data, including Trading Models, Trading Platforms, and email data for other Firm-1 employees, from Firm-1's system to an external third-party software development site. (Indictment ¶ 5). Zhang installed on Firm-1's system computer code designed to send the data through a Firm-1 backup server located in this District. (Indictment ¶ 6).

On September 13, 2017, a grand jury sitting in this District returned the Indictment, which charges Zhang in four counts. Count One charges Zhang with wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2. Count Two charges Zhang with computer fraud, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B), and 2. Count Three charges Zhang with aggravated identity theft, in violation of Title 18, United States Code, Sections 1028A(a)(1), (b), (c)(4), (c)(5), and 2. Count Four charges Zhang with theft of trade secrets, in violation of Title 18, United States Code, Sections 1832 and 2.

B. The Search Warrants

The defendant moves to suppress evidence obtained pursuant to five sets of judicially authorized search warrants:

1. The First Google Search Warrant and the First GitLab Search Warrant

On March 31, 2017, United States Magistrate Judge James C. Francis IV authorized two search warrants pursuant to the Stored Communications Act: one for any Google account associated with the email address zhang.zhengquan@gmail.com or the Google voice number 646-535-8168 (the "First Google Search Warrant"), and the second for any account associated with the name "Gitlabfan" maintained by GitLab, a third-party online Git repository (the "First GitLab Search Warrant"). (Def. Ex. A-2 (Google warrant); Gov't Ex. A (GitLab warrant)).[1]

The Government submitted a single Affidavit of FBI Special Agent Michael DeNicola in support of both warrants. (Def. Ex. A-1). The Affidavit attached and incorporated by reference an unsigned version of a complaint charging Zhang with a single count of theft of trade secrets based on allegations substantially similar to those later alleged in the Indictment. At the same time that Magistrate Judge Francis signed the two warrants, he also signed the complaint and a warrant for Zhang's arrest. (Docket 1).[2]

2. The Premises Search Warrant

On April 6, 2017, in anticipation of Zhang's imminent arrest (which in fact occurred the next day), the Government sought a warrant, pursuant to Federal Rule of Criminal Procedure 41, to search the premises of Zhang's residence located in the Northern District of California. On that

[1] Zhang did not include a copy of the First GitLab Search Warrant as an exhibit to his motion. The Government attaches a copy of the warrant as Exhibit A to this memorandum.

[2] On April 3, 2017, the Government submitted an amended complaint to correct an error in the caption of the complaint. The caption of the original complaint listed the statute violated as 18 U.S.C. § 1030, which the amended complaint corrected to 18 U.S.C. § 1832. United States Magistrate Judge Andrew J. Peck signed the amended complaint. (Docket 3). The body of the original complaint and the body of the amended complaint are identical. For the sake of simplicity, this memorandum will hereinafter refer to both versions as the "Complaint."

date, United States Magistrate Judge Nathanael M. Cousins authorized the warrant (the "Premises Search Warrant"). (Def. Ex. B-2). The Government submitted an Affidavit of FBI Special Agent Andrew Munn in support of the warrant. (Def. Ex. B-1). The Affidavit attached and incorporated by reference the Complaint.

3. The Second GitLab Search Warrant

On April 11, 2017, United States Magistrate Judge James L. Cott authorized a search warrant pursuant to the Stored Communications Act for any GitLab account associated with the name "fungitlab" (the "Second GitLab Search Warrant"). (Def. Ex. C-2). The Government submitted an Affidavit of FBI Special Agent Paul Bernardi in support of the warrant. (Def. Ex. C-1). The Affidavit attached and incorporated by reference both the Complaint and the Affidavit of Special Agent DeNicola in support of the First Google Search Warrant and the First GitLab Search Warrant.

4. The Second Google Search Warrant, the GitHub Search Warrant, and the Atlassian Search Warrant

On April 20, 2017, United States Magistrate Judge Debra Freeman authorized three search warrants pursuant to the Stored Communications Act: one for any Google account associated with four email addresses (student.northwestern@gmail.com, registerwebsite@gmail.com, god.roger.federer@gmail.com, and ibpricealert@gmail.com) (the "Second Google Search Warrant"); a second for any account associated with the name "Githubfun" maintained by GitHub, a third-party online Git repository (the "GitHub Search Warrant"); and a third for any account associated with the name "JimGreen" maintained by Atlassian, which runs a third-party online Git repository named BitBucket (the "Atlassian Search Warrant"). (Def. Ex. D-2 (Google warrant), D-3 (GitHub warrant), D-4 (Atlassian warrant)). The Government submitted a single Affidavit of

FBI Special Agent William McKeen in support of all three warrants. (Def. Ex. D-1). The Affidavit attached and incorporated by reference the Complaint.

On May 30, 2017, Zhang executed a consent for the Government to search three electronic devices seized during the search of his residence pursuant to the Premises Search Warrant as well as a consent for the Government to assume the online identity and search various online accounts of Zhang. (Def. Ex. F). Zhang also agreed, in a separate letter agreement dated May 26, 2017 and signed by him and his counsel on May 30, 2017 (the "May 26, 2017 Letter Agreement"), that the Government "may use the data obtained from the searches of the devices and online account (the 'seized data') in furtherance of the investigation and prosecution of this case without limitation." (*Id.*). Zhang agreed in the May 26, 2017 Letter Agreement "not to assert any claim that the Government is bound by the Northern District of California's search protocol for electronic devices," while the Government agreed not to assert that Zhang had waived "any right [he] may have to challenge the validity of the search warrants obtained by the Government as of this date." (*Id.*).[3]

5. The LinkedIn Search Warrant and the Third Google Search Warrant

On September 21, 2017, Magistrate Judge Francis authorized two search warrants pursuant to the Stored Communications Act: one for any Google account associated with three email addresses (zhang.zhengquan@gmail.com, god.roger.federer@gmail.com, and ibpricealert@gmail.com) (the "Third Google Search Warrant"); and a second for any LinkedIn account associated with certain URLs (the "LinkedIn Search Warrant"). (*See* Def. Ex. E-2

[3] The Government does not understand Zhang's motion to suppress to be making any argument beyond "the validity of the search warrants." To the extent, however, that his motion is construed to go beyond challenging the validity of the search warrants, or he makes such an argument now or later in the proceeding, the Government reserves the right to assert a waiver argument.

(LinkedIn warrant), E-3 (Google warrant)). The Government submitted a single Affidavit of Special Agent McKeen in support of both warrants. (Def. Ex. E-1). The Affidavit attached and incorporated by reference the Complaint, the Indictment, the Affidavit of Special Agent DeNicola in support of the First Google Search Warrant and the First GitLab Search Warrant, and the Affidavit of Special Agent McKeen in support of the Second Google Search Warrant, the GitHub Search Warrant, and the Atlassian Search Warrant.

On January 11, 2018, Zhang purported to "withdraw all waiver and consent provided pursuant to the May 26, 2017 Letter and attachments." (Def. Ex. F).[4]

II. Argument

A. Applicable Law

1. Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. Probable cause "is a fluid concept" turning "on the assessment of probabilities in particular factual contexts," and as such is not "readily, or even usefully, reduced to a neat set of legal rules." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Rather, probable cause is a "flexible, common-sense standard" that requires a case-by-case analysis of the totality of the circumstances. *Texas v. Brown*, 460 U.S. 730, 742 (1983); *see also Gates*, 462 U.S. at 230. In evaluating probable cause in any given case, a judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Falso*,

[4] Zhang's attempt to withdraw his previously given consent on the eve of his suppression motion, long after the searches of the devices and online accounts for which he gave consent, should be rejected.

544 F.3d at 117 (quoting *Gates,* 462 U.S. at 238). In close cases, where the existence of probable cause is in doubt, resolution "should be largely determined by the preference to be accorded to warrants." *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (internal quotation marks omitted). Moreover, "a court reviewing a challenged warrant—whether at the district or appellate level—must accord considerable deference to the probable cause determination of the issuing magistrate." *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (internal quotation marks omitted); *see also United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993) ("A reviewing court must accord substantial deference to the finding of an issuing judicial officer that probable cause exists. . . . The reviewing court's determination should be limited to whether the issuing judicial officer had a substantial basis for the finding of probable cause.") (citations omitted).

2. Particularity

"The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one particularly describing the place to be searched and the persons or things to be seized." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (internal quotation marks omitted). The particularity requirement of the Warrant Clause, which is distinct from the probable cause requirement, "guards against general searches that leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized." *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990).

"To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements." *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017). It must (i) "'identify the specific offense for which the police have established probable cause,'" (ii) "'describe the place to be searched,'" and (iii) "'specify the items to be seized by their relation to designated crimes.'" *Id.* (quoting *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013)). "The Fourth Amendment does not require a perfect description of the data to be searched and seized." *Id.* at 100. Rather, the

requirement is satisfied if the warrant, including its attachments, enables the executing officer to ascertain and identify with reasonable certainty those items that the magistrate judge has authorized him or her to seize. *See Groh v. Ramirez*, 540 U.S. 551, 557-59 (2004); *United States v. Rosa*, 626 F.3d 56, 58 (2d Cir. 2010).

The crime or crimes under investigation generally should be apparent from the face of the warrant; a warrant cannot, for example, call for seizure of all "records," or all evidence "relating to the commission of a crime," without further particularization. *United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (warrant permitting seizure of all "papers," "records," and other items, without any "more particular limiting language" or tethering "to particular crimes," was insufficiently particularized), *abrogated on other grounds by Groh*, 540 U.S. 551; *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992); *see also Galpin*, 720 F.3d at 445 ("[A] warrant must identify the specific offense for which the police have established probable cause."); *United States v. Vilar*, No. S3 05 Cr. 621 (KMK), 2007 WL 1075041, at *22 (S.D.N.Y. Apr. 4, 2007) ("[W]arrants are generally found to be insufficiently particular where 'nothing on the face of the warrant tells the searching officers for what crime the search is being undertaken.'" (quoting *George*, 975 F.2d at 76)).

However, a warrant for seizure of "all evidence" of a given crime or crimes is sufficiently particular if it offers a list of illustrative items. *See Riley*, 906 F.2d at 844-45 (warrant containing list of illustrative items to seize was sufficiently particular notwithstanding provision allowing, as well, seizure of "other items that constitute evidence of the offenses" identified); *United States v. Young*, 745 F.2d 733, 759-60 (2d Cir. 1984) (warrant allowing seizure of listed items plus "other evidence of" the specified crimes was sufficiently particular); *United States v. Lustyik*, 57 F. Supp. 3d 213, 227-28 (S.D.N.Y. 2014) (warrant permitting seizure of all "evidence, fruits, or

instrumentalities" of specified crimes was sufficiently particular because it contained "an illustrative list of items to be seized," even though illustrative list was preceded by phrase "including but not limited to"); *United States v. Jacobson*, 4 F. Supp. 3d 515, 524 (E.D.N.Y. 2014) ("[R]eference to particular offenses and the use of an illustrative list of items to seize sufficiently particularized the warrants."). The requirement is satisfied if the warrant, including its attachments, enables the executing officer to ascertain and identify with reasonable certainty those items that the magistrate judge has authorized him or her to seize. *See Groh*, 540 U.S. at 557-59; *Rosa*, 626 F.3d at 58.

A warrant may leave some matters to the discretion of the executing officer. "Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment as to whether a particular document falls within the described category." *Riley*, 906 F.3d at 845. Moreover, "[c]ourts tend to tolerate a greater degree of ambiguity where law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant." *Young*, 745 F.2d at 759. Indeed, "where a particularly complex scheme is alleged to exist, it may be appropriate to use more generic terms to describe what is being seized." *United States v. Gotti*, 42 F. Supp. 2d 252, 274 (S.D.N.Y. 1999) (citing *United States v. Regan*, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) ("The degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity investigated.")).

3. Overbreadth

The probable cause and particularity requirements intersect in the doctrine of overbreadth. As to each category of evidence identified for seizure in the warrant, there must exist probable cause to believe it is relevant to the investigation at issue. *See Galpin*, 720 F.3d at 448; *Lustyik*, 57 F. Supp. 3d at 228. "Thus, a warrant is overbroad if its 'description of the objects to be seized . . . is broader than can be justified by the probable cause upon which the warrant is based.'" *Id.* (quoting *Galpin*, 720 F.3d at 446); *see also United States v. Hernandez*, No. 09 Cr. 625 (HB), 2010 WL 26544, at *8-*9 (S.D.N.Y. Jan. 6, 2010) (framing overbreadth inquiry as "whether the magistrate judge authorized search warrants that were constitutionally overbroad because they provided for the seizure of items for which there is no probable cause"). Naturally, the broader the crime or crimes under investigation, the broader the categories of documents and records that may properly be seized. *See, e.g.*, *Jacobson*, 4 F. Supp. 2d at 522 (breadth of warrant was justified because "the crimes under investigation were complex and concerned a long period of time, not simply one or two dates of criminal activity"); *United States v. Levy*, No. 11 Cr. 62 (PAC), 2013 WL 664712, at *8 (S.D.N.Y. Feb. 25, 2013) (broad warrant with no timeframe limitation was justified by breadth and complexity of fraud described in underlying affidavit); *United States v. Dupree*, 781 F. Supp. 2d 115, 149 (E.D.N.Y. 2011) ("The nature of the crime . . . may require a broad search," such as where "complex financial crimes are alleged"); *Hernandez*, 2010 WL 26544, at *9 (broad warrant with no timeframe limitation justified by complexity of investigation).

4. Good Faith

Even if a warrant lacks probable cause or particularity, or is overbroad, "[t]he fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). Rather, the exclusion of evidence obtained in violation of the Fourth Amendment is a "prudential" remedy, crafted by the Supreme

Court "to compel respect for the constitutional guaranty." *Davis v. United States,* 564 U.S. 229 (2011) (internal quotation marks omitted). Neither a "personal constitutional right" nor a means to "redress the injury" of an unconstitutional search, the exclusionary rule is designed to deter future Fourth Amendment violations. *Id.* (internal quotation marks omitted). Because the remedy exacts a heavy toll on the justice system, however, the exclusionary rule should only be applied where law enforcement "exhibit[s] deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *United States v. Raymonda*, 780 F.3d 105, 117-18 (2d Cir. 2015) (quoting *United States v. Stokes*, 733 F.3d 438, 443 (2d Cir. 2013)). In fact, exclusion should be a "last resort" rather than a "first impulse." *Id.* Thus, suppression will not be warranted where the evidence at issue was "obtained in objectively reasonable reliance on a subsequently invalidated search warrant." *United States v. Leon*, 468 U.S. 897, 922 (1984); *see also Falso*, 544 F.3d at 117; *Raymonda*, 780 F.3d at 118.

Although the burden is on the Government to establish good faith, "[s]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Leon*, 468 U.S. at 922 (citations and internal quotation marks omitted); *see also United States v. Rickard*, 534 F. App'x 35, 37 (2d Cir. 2013) ("Most such searches will be upheld."). Only if one of the following circumstances obtains will the searching officers' good faith not have been established:

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Clark, 638 F.3d at 100 (quotation marks and citations omitted). The "so lacking in indicia of probable cause" concern "most frequently arises when affidavits are bare bones, *i.e.*, totally devoid of factual circumstances to support conclusory allegations." *Id.* at 103. "At the opposite end of the spectrum are cases in which a defective warrant issued based on an affidavit providing detailed factual allegations in support of probable cause." *Id.* "Such cases almost invariably demonstrate reasonable reliance." *Id.*

Where the warrant is defective for lack of particularity rather than probable cause, the good-faith analysis focuses on whether the officers' execution of the warrant reflected a reasonable belief that they were operating within the confines of the Fourth Amendment because they executed the search in a manner tethered to the underlying affidavit and its statement of probable cause. *See Rosa*, 626 F.3d at 64 (although facial validity of the warrant must be assessed independent of unattached affidavit, affidavit was "still relevant to our determination of whether the officers acted in good faith," to the extent the officers searched for evidence based on the affidavit's probable cause statement). If (i) the affidavit identifies the crimes being investigated and the evidence sought, (ii) the agent who swore out the affidavit participated personally in the execution of the search, and (iii) the team relied on "their knowledge of the investigation and the contemplated limits" set forth in the affidavit, then suppression should not be ordered notwithstanding a valid particularity challenge. *See id.* at 64-66 (applying good-faith exception to affirm denial of suppression motion where face of warrant allowed blanket search of "computer equipment" and other electronic devices for anything "which would tend to identify criminal conduct" of any kind). Even where searching officers' reliance on the warrant was unreasonable for one or more of the reasons identified above, however, suppression still will not be warranted absent deliberate, culpable conduct: "To trigger the exclusionary rule, police conduct must be

sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144; *see also Rosa*, 626 F.3d at 64, 66.

B. Discussion

1. The First Google Search Warrant and the First GitLab Search Warrant Were Supported by Probable Cause, Were Sufficiently Particular, and Were Not Overbroad

(a) Probable Cause. Zhang concedes that probable cause supported the First GitLab Search Warrant. (Mem. 19). Zhang argues, however, that probable cause was lacking for the First Google Search Warrant in several specific ways. None of his arguments has any merit.

Zhang contends that the DeNicola Affidavit in support of these warrants failed to establish a connection between the crimes and the Google email address (zhang.zhengquan@gmail.com) or voice number (646-535-8168) targeted in the First Google Search Warrant. (Mem. 18-19). To the contrary, the Affidavit readily established probable cause of such a connection. The Affidavit first set forth detailed facts showing that Zhang personally used the email address and voice number. (Def. Ex. A-1 ¶¶ 12(a)-(c), 13).[5] The Affidavit also set forth that in Special Agent DeNicola's experience, the personal electronic accounts of cybercriminals often have relevant evidence of their crimes, including information about other electronic accounts used in the crimes and evidence of the planning and execution of the crimes. (*Id.* ¶ 11). And the Affidavit set forth facts showing that Zhang in fact used the email address and the voice number to partially confess his crimes to

[5] Zhang objects that some of these facts simply establish innocent use of the email address and voice number. (Mem. at 18). The Government does not contend otherwise. These facts are nevertheless relevant because they establish probable cause that Zhang personally used the email address and voice number. The fact of personal use then combines with Special Agent DeNicola's experience-driven testimony that cybercriminals often have evidence of their crimes in their personal electronic accounts and the specific instances of Zhang's actually using the accounts to communicate with his employer about the crimes.

his supervisor and then to inquire about his employment status. (*Id.* ¶¶ 12(d), 13; *see also* Complaint ¶ 6(f)-(g)). These facts established probable cause that Zhang's Google accounts would contain evidence of the subject offenses.

Zhang attempts to invalidate Paragraph 11 of the Affidavit, which, as noted above, set forth that in Special Agent DeNicola's experience, the personal electronic accounts of cybercriminals often have relevant evidence of their crimes, including information about other electronic accounts used in the crimes and evidence of the planning and execution of the crimes. Zhang questions Special Agent DeNicola's experience and qualifications by misleadingly suggesting that his only qualifications are his participation in "'several investigations into various forms of online criminal activity' and an undisclosed number of execution of search warrants." (Mem. 17 (quoting Def. Ex. A-1 ¶ 1)).

But Special Agent DeNicola's qualifications went beyond Zhang's selective quotations. As set forth in the Affidavit, Special Agent DeNicola had been an FBI Special Agent for nearly two years at the time he swore out the Affidavit; he had spent that entire tenure in the specialized "computer intrusion squad" of the FBI's New York Field Office; and he had "participated in numerous investigation of computer crimes, among other federal crimes." (Def. Ex. A-1 ¶ 1). One subset of those numerous computer-crime investigations was the category of "investigations into various forms of online criminal activity" mentioned by Zhang. (*Id.*). That online criminal activity included "various fraudulent schemes perpetrated through the use of the Internet," and as a result Special Agent DeNicola was "familiar with the ways in which such crimes are commonly conducted." (*Id.*). Finally, Special Agent DeNicola did not merely participate in the "execution of search warrants" (Mem. 17), but he participated in the execution of search warrants "involving electronic evidence relating to [his] investigations, including email accounts." (Def. Ex. A-1 ¶ 1).

It was reasonable for the magistrate judge to conclude that these experiences readily established that Special Agent DeNicola had the experience and expertise to testify that the personal electronic accounts of cybercriminals often have relevant evidence of their crimes, including information about other electronic accounts used in the crimes and evidence of the planning and execution of the crimes.[6]

(b) Particularity/Overbreadth. Zhang's particularity and overbreadth arguments are likewise meritless. The warrants are sufficiently particular as to the subject offenses, the place to be searched, and the items to be seized, and are not overbroad.

(i) Offense. The First Google Search Warrant and the First GitLab Search Warrant each includes an Attachment, Section III of which specifically authorizes the search for evidence, fruits, and instrumentalities of "fraud and related activity in connection with computers, including unauthorized access or access exceeding authorization of computers, in violation of Title 18, United States Code, Section 1030; wire fraud, in violation of Title 18, United States Code, Section 1343; theft of trade secrets, in violation of Title 18, United States Code, Section 1832; and conspiracy to do the same, in violation of Title 18, United States Code, Section 371; among other statutes." (Def. Ex. A-2 § III (ZZ_000060); Gov't Ex. A § III (ZZ_000066)).

[6] Indeed, Special Agent DeNicola's testimony regarding the personal electronic accounts of cybercriminals was borne out by the results of the search warrant, which included evidence that Zhang used his personal email address to set up other electronic accounts involved in the crimes and evidence of Zhang's planning and execution of the crimes. (*See*, *e.g.*, Def. Ex. D-1 ¶ 17 (noting zhang.zhengquan@gmail.com account was used to register GitHub account); Def. Ex. E-1 ¶ 13 (noting zhang.zhengquan@gmail.com account was used by defendant to conduct research into how to reverse engineer trading algorithms and research potential jobs for algorithmic and high-frequency trading strategies, which suggests the defendant's motive for stealing Firm-1's data and the ways in which he intended to use it); Def. Ex. E-1 ¶ 16(b) (noting communications found in zhengquan.zhang@gmail.com account between Zhang and others on LinkedIn regarding Zhang's pursuit of other jobs while he was actively stealing data from Firm-1).

Zhang complains that this description of the subject offenses encompasses "a myriad of offenses that clearly had no relationship to the offenses at issue" in this case, and offers the example of child pornography. (Mem. 19). But that is a strawman—no reasonable person would understand a warrant authorizing a search for evidence of the specific enumerated offense of computer fraud and hacking, wire fraud, theft of trade secrets, and conspiracy to commit those offenses—complete with statutory citations for each—to also implicitly encompass child pornography. Furthermore, just three subparagraphs below the above-quoted list of specified offenses is a more detailed description of the sought-after evidence for each offense: for Section 1030, "efforts made to obtain user credentials or passwords, infrastructure used in furtherance of those efforts, and evidence of what data was sought"; for wire fraud, "artifices or devices designed to obtain money or property"; and for theft of trade secrets, "motive or the efforts made to monetize the items, or ways that means to guard the trade secret were circumvented." (Def. Ex. A-2 § III(c) (ZZ_000060); Gov't Ex. A § III(*l*) (ZZ_000067)). These additional details further confirm that the specific offenses would not reach child pornography.[7]

Zhang's particularity objection regarding the subject offenses ultimately appears to boil down to the warrant's use of the phrase "among other statutes" after the list of specific offenses and statutes. (Mem. 20). But Zhang fails to cite—and the Government is not aware of—any case holding that the use of such a phrase somehow constitutionally nullifies the listing of specific offenses that ordinarily satisfies the particularity requirement. Furthermore, search warrants that have been invalidated for insufficiently particularizing the subject offenses were far less specific

[7] Zhang also complains that the list of specified offenses encompasses "virtually any other federal offense under the wire fraud statute that in any way involved the use of the computer." (Mem. 19). This is a peculiar objection because wire fraud involving the use of a computer is in fact one of the charges against the defendant in this case. (Indictment ¶¶ 3-7).

than the warrants here, for they failed to specify *any crime at all* or alluded broadly to *all state or federal law*. *See Galpin*, 720 F.3d at 447 (warrant authorized search of evidence of "NYS Penal Law and or Federal Statutes"); *Rosa*, 626 F.3d at 58, 62 (warrant failed to set forth "the nature of the suspected criminal activity"); *Bianco*, 998 F.2d at 1116 (warrant "made no mention of any criminal statute or criminal conduct"); *George*, 975 F.2d at 76 ("Nothing on the face of the warrant tells the searching officers for what crime the search is being undertaken.").

(ii) Place to Be Searched. Zhang does not challenge the particularity of the place to be searched.

(iii) Items to Be Seized. Section III of the Attachment to the First Google Search Warrant and the First GitLab Search Warrant authorizes the search for "evidence, fruits, and instrumentalities" of the subject offenses. Section III then specifies that such evidence "includ[es] the following" and goes on to enumerate nine categories that are examples of such evidence. (Def. Ex. A-2 § III (ZZ_000060-61); Gov't Ex. A § III (ZZ_000066-68)). Such a list of illustrative enumerated categories of evidence, which clearly modifies and is tethered to the specific crimes being investigated, is sufficiently particularized under the Fourth Amendment. *See, e.g.*, *Riley*, 906 F.2d at 844-45; *Young*, 745 F.2d at 759-60, *Lustyik*, 57 F. Supp. 3d at 227-28.

Zhang specifically objects to five of the nine categories in the list in what appears to be an overbreadth argument. (Mem. 20). None of the objections has any merit:

- Evidence regarding the "use of the Subject Accounts" (Def. Ex. A-2 § III(a); Gov't Ex. A § III(j)) is necessary for purposes of attribution of a particular piece of online infrastructure, such as an email account or a Git repository account, to a particular individual, such as Zhang or a potential co-conspirator.

- "[E]vidence relating to the use of the Internet, email, computers, or other electronic devices in furtherance of the Subject Offenses" (Def. Ex. A-2, § III(d); Gov't Ex. A § III(m)) can be (and in this case, was) found in email accounts used by Zhang (which identified other online infrastructure, including IP addresses, accounts, websites, and search engines, that he used in furtherance of his crimes), as well as

his use of the Google Voice account to communicate with a Firm-1 employee in partial confession of his criminal conduct;

- Evidence regarding "other fraudulent activities," was not "unbridled" (Mem. at 20), but instead modified the phrases "[e]vidence relating to the Internet, email, computers, or other electronic devices," a category of evidence pertaining to the means and methods of the specified offenses at issue, and "[e]vidence relating to the use of financial accounts and transactions," a narrow category of evidence which would identify "the means and methods used to obtain the accounts and the funds therein, and the how the transactions were undertaken." (Def. Ex. A-2 § III(e)); Gov't Ex. A § III(n)).

- The phrase "online infrastructure" (Def. Ex. A-2, Section III(f); Gov't Ex. A. § III(o)) is oftentimes used by investigators in the cybercrime context to include hardware, devices, software, and accounts requisite to commit cybercrimes, *i.e.*, the "requisite infrastructure acquired to execute the crimes." (Def. Ex. A-1 ¶ 11).

- "[A]ny other evidence of the Subject Offenses" is a category of evidence that has been repeatedly approved by courts in this Circuit as being sufficiently particular. *See, e.g., Riley*, 906 F.2d at 844-45; *Young*, 745 F.2d at 759-60; *United States v. Patel*, 16 Cr. 798 (KBF), 2017 WL 3394607, at *4 (S.D.N.Y. Aug. 8, 2017) (concluding that search warrant that enumerated "evidence of crime" as category to be seized was sufficiently particular and not overbroad).

Zhang claims that the search warrants here are less particularized and more overbroad than the warrants at issue in *United States v. Patel*, a case in which the Court denied a particularity and overbreadth challenge. (Mem. 15-16). Yet a comparison of the categories of evidence in the *Patel* Search Warrant (including "evidence of crime," "preparation for crime," "state of mind," "user identity," "timeline," "geographic location of user, computer, or device," "identities and locations of co-conspirators," "location of other evidence," and "passwords or other information needed to access user's computer or other online accounts" (Def. Ex. G)) and the categories in the search warrants in this case are only distinguishable in that the search warrants in this case contain more detail about the types of evidence sought. This additional detail as to the types of evidence that should be seized by law enforcement does not render the warrants here insufficiently particular or improperly overbroad.

Finally, with respect to the First GitLab Search Warrant, Zhang objects that the warrant "clearly related to an email account or a computer and not a document repository." (Mem. 21). This appears to be a reference to the Attachment being titled "Email Search Attachment A." But the body of the Attachment itself makes clear that the warrant is for a Git repository and not an email account. (Gov't Ex. A-3). The minor error in the Attachment's title does not constitute a particularity or overbreadth problem.

2. The Premises Search Warrant Was Supported by Probable Cause, Was Sufficiently Particular, and Was Not Overbroad

Zhang concedes that the Premises Search Warrant was sufficiently particular, and he does not object to any specific category of items to be seized as overbroad. (Mem. 26). Zhang instead asserts that probable cause was lacking for the Premises Search Warrant, principally because the Munn Affidavit in support of the warrant purportedly fails to establish that Zhang used a computer located at his residence to engage in the crimes. (Mem. 25).

Of course, the relevant question is not whether Zhang used a computer at his residence to engage in the crimes, but rather whether there was probable cause to believe that the computer would contain evidence of the crimes. Based on the following facts, the Affidavit indeed established probable cause to believe that computers and electronic devices located at Zhang's residence would contain evidence of the subject offenses. (Zhang's specific objections to certain facts in the Affidavit are addressed in the footnotes.)

- Zhang had used two different computers—his Firm-1 issued laptop, as well as a personal computer—to remotely access Firm-1's computer network from the same IP address in Santa Clara, California (the "Santa Clara IP Address"), the town in which Zhang lived. (Def. Ex. B-1 ¶¶ 11-12).

- These two computers were used to access Firm-1's network outside of normal business hours on weekdays, including late at night and also on the weekends,

during the time period that Zhang was engaged in the crimes (December 2016 to March 2017). (Def. Ex. B-1 ¶ 12; Complaint ¶ 1).[8]

- After Zhang's unauthorized access had been detected by Firm-1 and his work access privileges had been terminated (*see* Complaint ¶ 5(e)), Zhang entered his office in San Jose late in the evening of Sunday, March 26, 2017, and deleted from Firm-1's computer network "various history files, logs, and directories evidencing the Subject Offenses" and then left his work laptop at Firm-1's San Jose office. (Def. Ex. B-1 ¶ 13).[9]

- Zhang then subsequently used another device (not his work laptop, which he had left at Firm-1's office) to send an email in which he admitted he had committed unauthorized access—which in and of itself is evidence of the crime at hand. (Def. Ex. B-1 ¶ 14).

- Based on his training and experience, Special Agent Munn, a cyber investigator,[10] explained that criminals involved in network intrusion and extrusions of data "commonly use a variety of types of computer infrastructure . . . both to code the requisite programs to successfully intrude . . . as well as to retrieve and store relevant data, such as stolen source code" and "often use their residence as a base of operations for a variety of reasons, including the times during which they

[8] Zhang objects that the Santa Clara IP Address was not specifically traced to Zhang's residence at the time. (Mem. 24-25). But there was other evidence establishing probable cause that the Santa Clara IP Address was associated with Zhang's residence, including the fact that Zhang's work computer accessed Firm-1's network from that IP address outside of normal business hours. That evidence also corroborated the cybersecurity firm retained by Firm-1 that had resolved the IP address to the town of Santa Clara, despite Zhang's protests to the contrary. (Mem. 24). Indeed, subpoena returns that the Government received after Zhang's arrest regarding the Santa Clara IP Address confirmed that the IP address from which Zhang's computers accessed the Firm-1 network was in fact the IP address associated with Zhang's residence. (*See, e.g.*, Def. Ex. D-1 ¶ 15 (noting Santa Clara IP Address as ending in .233, and assigned to Zhang at his residence where he was arrested on April 7, 2017)).

[9] Zhang points to his destruction of evidence at Firm-1's office as proof that he did not use a personal computer from his residence to engage in the crime. (Mem. 25). But the fact that Zhang did not log in remotely from his residence *after Firm-1 had terminated his network access* does not undermine at all the fact that he had previously logged in remotely from his residence using a personal computer.

[10] Zhang questions Special Agent Munn's reliance in the Affidavit on information from another FBI special agent (Mem. 24), but Zhang calls no specific fact into question based on this reliance.

conduct their criminal activity, and the fact that residences can provide for a secure and reliable internet connection" (*see* Def. Ex. B-1 ¶ 16).[11]

These facts establish probable cause that Zhang used a personal computer from his residence to access Firm-1's network during the multi-month time period when he was engaged in the subject offenses, and also that he used a personal electronic device to email his employer with a partial confession of his crimes. Thus, the Affidavit established probable cause that personal computers or electronic devices found at Zhang's residence would contain evidence of those crimes.[12]

3. The Second GitLab Search Warrant Was Supported by Probable Cause, Was Sufficiently Particular, and Was Not Overbroad

Zhang summarily asserts that probable cause was lacking for the Second GitLab Search Warrant. (Mem. 21). This claim ignores his concession that probable cause supported the First GitLab Search Warrant. (Mem. 19). The reason that the Government sought the Second GitLab Search Warrant was because, upon further review of the data, GitLab had indicated to the Government that data that had previously been associated with the "gitlabfan" account (targeted in the First GitLab Search Warrant) was now associated with the "fungitlab" account (targeted in the Second GitLab Search Warrant). (Def. Ex. C-1 ¶¶ 10-13). Thus, if there was probable cause

[11] Zhang contends that this fact is undermined by the fact that Zhang went into the office late in the evening on Sunday, March 26, 2017. (Mem. 25). Again, the fact that Zhang went into the office rather than log in remotely from his residence *after Firm-1 had terminated his network access* does not undermine at all the fact that cybercriminals often use their residence as a base of operations.

[12] Zhang notes the Complaint's allegation that the "computer code that ZHANG wrote to exfiltrate data to the Development Website was designed to route all of the data through Firm-1's backup proxy server in Purchase, New York." (Mem. 25). The Government expects that the evidence at trial will establish that Zhang deliberately circumvented Firm-1's security measures by routing the data he stole from Firm-1 through the use of a proxy server that was located in the Southern District of New York, and that subsequent to his having exfiltrated the data to the third-party Git repositories, he then downloaded the data to his home devices. The Government's subsequent review of the evidence established that Firm-1's proprietary data was found on at least three devices seized at Zhang's residence, consistent with Zhang having exfiltrated the data from Firm-1 to third-party Git repositories, and then downloading that data to his home devices.

for the First GitLab Search Warrant (as Zhang concedes), there was necessarily probable cause for the Second GitLab Search Warrant.

Zhang advances particularity and overbreadth claims for the Second GitLab Search Warrant "for the same reasons" he asserts for the First Google Search Warrant and the First GitLab Search Warrant. (Mem. 21). These claims fail for the reasons discussed above.

4. The Second Google Search Warrant, the GitHub Search Warrant, and the Atlassian Search Warrant Were Supported by Probable Cause, Were Sufficiently Particular, and Were Not Overbroad

Zhang once again raises the same probable cause, particularity, and overbreadth challenges, this time with respect to the Second Google Search Warrant, the GitHub Search Warrant, and the Atlassian Search Warrant. (Mem. 21-22). They fail for the same reasons discussed above.

Zhang does, however, raise an argument specific to these warrants. These warrants added securities fraud to the subject offense, and Zhang argues that the McKeen Affidavit in support of these warrants failed to establish probable cause to believe that Zhang committed securities fraud and that evidence of securities fraud would be found in the various electronic accounts covered by these warrants. (Mem. 21-22).

Zhang's claim has no merit, because the Affidavit established such probable cause with respect to securities fraud. The Affidavit set forth that by virtue of his employment at Firm-1 (as a Series 99 Operations Professional within a FINRA regulated broker-dealer), Zhang was obligated to disclose to Firm-1 all of his trading accounts, as well as those of his immediate family, including his wife. Nevertheless, review of subpoena returns from an online brokerage firm ("Firm-2") revealed that although Zhang had previously held an account at Firm-2 that he had disclosed to Firm-1, he failed to disclose an account at Firm-2 held in the name of Zhang's wife, which account was associated with Zhang's personal email accounts. (*See* Def. Ex. D-1 ¶ 18). Zhang's failure to

disclose to Firm-1 the existence of a Firm-2 trading account in his wife's name, for which he had account access given that it was associated with his personal email accounts, establishes probable cause that the securities account was used in a deceptive, manipulative, or fraudulent manner. Thus, these facts were sufficient to establish that, "given all of the circumstances . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Falso*, 544 F.3d at 117.

In any event however, assuming *arguendo* that the Affidavit failed to establish probable cause that Zhang engaged in securities fraud (and that good faith cannot be established), any evidence of Zhang's use of or control over trading accounts would also be properly searched for and seized as evidence of the other subject offenses specified in the warrants and affidavit. Specifically, the Government expects that, in any trial against Zhang, it will put forth evidence that Zhang attempted to use the data he stole from Firm-1 to reverse engineer the source code and understand the mechanics behind the trading strategies employed at Firm-1, such that he might be able to market himself as a quantitative analyst (like the individual Firm-1 employees from whom he stole source code and email data). Therefore, any evidence that relates to Zhang having participated in securities fraud would also be evidence of a motive for Zhang having stolen Firm-1's proprietary trading source code for his own personal use or gain. As such, Zhang cannot assert that any evidence that is relevant to a securities fraud violation would not also be relevant to the other subject offenses.

5. The LinkedIn Search Warrant and the Third Google Search Warrant Were Supported by Probable Cause, Were Sufficiently Particular, and Were Not Overbroad

Zhang next challenges probable cause, particularity and overbreadth with regard to the LinkedIn Search Warrant and the Third Google Search Warrant. These challenges fail in the first

instance for the same reasons as set forth above in the context of the other search warrants discussed above.

Zhang also asserts that probable cause for these specific warrants was lacking because none of the evidence seized pursuant to the prior search warrants "confirm[ed] that the accounts were used in furtherance of the subject offenses or even suggest criminal activity." (Mem. 22). Zhang fundamentally misunderstands the evidence and the probable cause inquiry:

- The fact that Zhang used the zhang.zhengquan@gmail.com account to correspond with his wife (Def. Ex. E-1 ¶ 13)—a fact that certainly helps conclude it is Zhang who controlled the account—is not the sole basis for probable cause. (*contra* Mem. 23). Rather, the relevant facts are that his wife shared non-public information with Zhang about a potential merger of a client of her employer (a venture capital firm) with another company. Zhang then attempted to research stock price movements of both companies at issue, as evidenced by the contemporaneous Google search history associated with the zhang.zhengquan@gmail.com account. (Def. Ex. E-1 ¶ 13(c)). The Government's investigation into what Zhang may have done with that information—including attempting to determine if Zhang had access to other trading accounts beyond those in his wife's name that he failed to disclose to Firm-1 or FINRA—is ongoing.

- Zhang's Google search for the phrase "reverse engineer trading strategy" and his subsequent review of websites relating to that search, including one relating to how to "reverse engineer a market-making algorithm (HFT)" (Def. Ex. E-1 ¶ 13(a))—the precise type of algorithmic trading that was employed by Firm-1—is evidence that helps to establish Zhang's motive. The fact that the Affidavit did not define "reverse engineer trading strategy," as Zhang suggests it should have, does not render the warrant invalid, as it is apparent that the magistrate judge understood what the phrase meant.

- Zhang's attempts to research other jobs in the industry—including ones for which he was not qualified, but were akin to positions for the employees from which Zhang stole data (Def. Ex. E-1 ¶ 13(b)), as well as his researching the term "fraud" in the context of immigration proceedings—all the while evidencing a strong concern regarding his ability to achieve permanent residency status, including after he was terminated from FINRA registration (*see* Def. Ex. E-1 ¶ 13(d))—constitute not only probable cause that the data sought would contain evidence of the subject offenses with which Zhang was charged, but also that the accounts might contain evidence of immigration or visa fraud.

These facts readily establish "circumstances" to conclude that "there is a fair probability that contraband or evidence of a crime" would be found within the accounts sought. *Falso*, 544

F.3d at 117. And again, assuming *arguendo* that the Affidavit failed to establish probable cause that Zhang engaged in securities fraud or immigration fraud (and that good faith cannot be established), any evidence of Zhang's use of or control over trading accounts, as well as his efforts to seek legal immigration status, would be relevant evidence of the other crimes with which he was charged. As discussed above, the Government expects that, in any trial against Zhang, it will put forth evidence that Zhang attempted to use the data he stole from Firm-1 such that he might be able to market himself as a quantitative analyst and seek employment outside of Firm-1, either by being sponsored for H1B status from another firm, or after receiving permanent residency status. As such, Zhang cannot assert that any evidence that is relevant to a securities fraud or immigration fraud violation would not also be evidence relevant to establish the other Subject Offenses.

6. Law Enforcement Agents Relied on the Warrants in Good Faith

This is a case where "the crimes under investigation were committed largely through computers [and online accounts] that there was probable cause to believe included the [computers and online accounts] at issue, and the search warrant application[s] gave ample basis for the issuing magistrate judges[s] to conclude that evidence related to" Zhang's unauthorized access and network exfiltration activity would exist on the digital devices stored at his home and his online accounts. *See Ulbricht*, 858 F.3d at 103-04. Thus, "given the nature of [Zhang's] crimes and their symbiotic connection to his digital devices [and online accounts]," the warrants were well within the bounds of "well-settled Fourth Amendment principles." *Id.*

But even if any of the challenged search warrants lacked probable cause, was insufficiently particular, or was overbroad, the evidence should not be suppressed because the law enforcement agents who executed the warrants reasonably relied on them in good faith. On five separate occasions, a total of four magistrate judges in this District and the Northern District of California issued five sets of search warrants based on affidavits sharing a core set of facts (*i.e.*, Zhang's

crimes). *See Leon*, 468 U.S. at 922 ("Searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." (citations and internal quotation marks omitted)). None of the circumstances undermining a finding of good faith reliance is present here. There is no allegation that the magistrate judges were "knowingly misled" or that the magistrate judges "wholly abandoned [their] judicial role"; nor were the applications here "so lacking in indicia of probable cause" or the warrants "so facially deficient" that the agents' reliance upon them was unreasonable. *See Clark*, 638 F.3d at 100 (internal quotation marks omitted).

Finally, this case is nothing like *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017), in which a combination of aggravating factors led the Court to conclude that the good-faith rule did not apply. *Wey* featured, for example, search warrants that did not identify the subject offenses; premises warrants that permitted the seizure of virtually any document related to the owner or occupant of the premises; law enforcement attempts to deem unresponsive materials responsive; and continued re-searching of seized electronic data for years to find new evidence. *Id.* at 398-409. None of those factors is present here.[13]

[13] Nor are the warrants in this case anything like the "catch-all" warrant in *United States v. Buck*, which lacked "any list of particular items or any other limiting language." 813 F.2d 588, 593 (2d Cir. 1987).

III. Conclusion

For the reasons set forth above, this Court should deny Zhang's motion to suppress in its entirety.

Dated: New York, New York
February 17, 2018

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: /s/
Eun Young Choi / Won S. Shin
Assistant United States Attorneys
(212) 637-2187 / 2226